Cassandra Crossing/ CCC2015: Il laptop di Snowden

(353) — Che trattamento viene riservato a una macchina che contiene dati top secret come quelli che Snowden ha consegnato al mondo? Una…

Cassandra Crossing/ CCC2015: Il laptop di Snowden

Figure 1:

(353) — Che trattamento viene riservato a una macchina che contiene dati top secret come quelli che Snowden ha consegnato al mondo? Una presentazione dal Chaos Communication Camp 2015.

11 set 2015—Cassandra ha trovato una piccola perla nel programma del Chaos Communication Camp di quest'anno: è andata ad ascoltare un talk senza troppa convinzione, ma questo si è poi rivelato interessantissimo. Anche perché, malgrado la sua brevità, racconta tutta la storia dell'inizio e dettagliatamente.

L'intervento, tenuto da Mustafa Al-Bassam e Richard Tynan, dal titolo "Come distruggere un laptop contenente materiale top secret" e dal sottotitolo "Cosa hanno fatto i servizi segreti alla copia del Guardian dei file di Snowden" (*How to Destroy a Laptop with Top Secrets: How did GCHQ do it to the Guardian's copy of Snowden's files?*) è stato presentato da due collaboratori del Guardian, il giornale di Greenwald, e riguardano il portatile che Snowden chiese a Greenwald di portare con sé per potergli consegnare i file "originali" del Datagate.

Come alcuni dei 24 informatissimi lettori ben sanno, non è che Greenwald fosse proprio una cima riguardo alla crittografia e alla sicurezza informatica, tant'è che il primo contatto tra i due, circa un anno prima, fallì proprio per l'incapacità di Greenwald di utilizzare difficili tecnologie come PGP e simili.

Per fortuna poi Snowden contattò Laura Poitras, che fece da "intermediario" e da mentore a Greenwald, ed alla fine il famoso incontro nella camera di albergo ebbe luogo, ed è immortalato nel film/documentario Citizen Four della stessa Poitras. Anche questo da vedere assolutamente!

Snowden chiese un portatile "Air Gapped", cioè un oggetto nuovo, comprato in un negozio scelto a caso, che non fosse mai stato connesso a nessun tipo di rete. "Separato dall'aria", appunto. In Citizen Four si vede anche la ripresa della consegna.

E' questo il portatile che tornò a Londra alla redazione del Guardian, ed è questo portatile che fu chiesto per vie non ufficiali dal GCHQ, cioè dai Servizi Segreti di Sua Maestà, che ne pretesero la consegna attraverso prima pressioni informali e poi minacce semi-formali.

Siccome i cittadini inglesi sono persone abbastanza serie, quindi la redazione di un giornale non è luogo che si possa violare impunemente, il Guardian ebbe il coraggio di rifiutare di consegnarlo.I servizi segreti avevano due ottimi motivi per volere il laptop.

Il primo, facile da intuire, è per sottoporlo ad un'analisi forense particolarmente raffinata che potesse fornire qualche elemento su Snowden, sulla sua posizione o sui suoi collaboratori…

Chessò il nome della rete wifi a cui si fosse per sbaglio collegato…

Il secondo, più banale ma altrettanto valido e per loro ineludibile, è per distruggere completamente una copia dei dati top secret del Datagate, benché fosse già stato comunicato dal Guardian al GCHQ che erano anche stati copiati altrove.

Fu trovato un accordo nel quale il Guardian accettava solo che il laptop fosse distrutto secondo le procedure formali in vigore al GHCQ, e che la distruzione sarebbe avvenuta alla presenza di tecnici del GCHQ ma sarebbe stata eseguita da tecnici del Guardian.

Una magnifica opportunità per imparare un sacco di cose.

Detto fatto, al Guardian è stato richiesto di mettere a disposizione una stanza chiusa, strumenti tipo morse, una levigatrice orbitale, un trapano a colonna, occhiali e mascherine di protezione.

I due tecnici del GCHQ che si sono presentati avevano tutti e due una clearance Top Secret, perché questo era richiesto dalle procedure per poter distruggere in maniera affidabile e certificata dei dati Top Secret.

Due, uno non basta.Esiste un documento del GCHQ che dovrebbe essere pubblico, ma appartiene a quella categoria di documenti pubblici che non ti danno mai, che spiega tutte queste procedure.

Il Guardian lo richiese e gli fu negato, ma vedi caso il manuale stesso faceva parte dei documenti consegnati da Snowden e così…

Per farla breve, qualsiasi procedura informatica di bonifica venga applicata ad un portatile che contenga dati top secret non ne cambia la sua classificazione, che rimane Top Secret.

Formattate a basso livello, utilizzate degausser sui dischi, cancellate e ricaricate tutti i firmware del computer e dei suoi subcomponenti, e tutto questo verrà giudicato comunque inefficace.

L'unico modo consentito per declassificare un portatile in maniera semplice è, non scherzo, tritarlo finemente in modo che la polvere ottenuta possa passare tutta attraverso un setaccio con maglia di tre millimetri.

Altrimenti, anche se ha contenuto un solo Byte di informazioni top secret, poi cancellate accuratamente, rimane un oggetto classificato top secret.

Riassumendo: consiglio a tutti coloro che appena appena capiscono un buon inglese di spendere 58 minuti della propria esistenza per ascoltare la presentazione illustrata al CCC.

Nel suo piccolo è altrettanto rivelatrice del Datagate stesso, perché apre una (piccola) finestra sul ruolo e sui limiti dell'informatica nel caso di trattamento di informazioni REALMENTE confidenziali.

Quindi Cassandra eviterà la fatica di fare un riassunto ad uso di chi non ha tempo, e si limiterà a cinque pillole scelte tra i contenuti del talk (quindi opinioni espresse dagli oratori).

- [una macchina che ha contenuto dati top secret non è considerata "bonificabile" con mezzi informatici;]
- [- la "bonifica" prevede la distruzione fisica, mirata a seconda del modello, di una serie di circuiti integrati inclusi RAM, BIOS, controllore tastiera, controllore touchpad, controllore alimentatore]
- [chi esegue queste operazioni dispone di informazioni assai dettagliate sui vari modelli di portatili;- i prodotti Apple sono considerati meno affidabili e meno verificabili e quindi soggetti a bonifiche più "severe";- esistono dettagliati manuali operativi nei vari servizi segreti (sembra molto simili tra i vari paesi) su come operare queste "bonifiche" di dati a seconda dei supporti che li contengono.]
- [A parte i primi due, gli altri "strani" componenti, poiché contengono memoria locale, possono essere usati da un "software atipico" (utente, criminale o di stato) per immagazzinare informazioni: questo sembra essere il motivo per cui vengono polverizzati.]
- [Pensare che persino il controllore della batteria possa essere usato per "esportare" informazioni non è tuttavia l'unica possibilità: un'altra ad esempio è che il normale e legittimo profilo dei consumi della batteria possa rivelare quando il portatile viene usato e magari la timezone dell'utente, ed i suoi eventuali spostamenti.]
- [Che non siano questioni da prendere sottogamba è confermato dal "pettegolezzo" che ad alcuni altissimi funzionari inglesi sia stato tritato l'iPhone personale perché, solo per ricaricarlo, l'avevano connesso per un attimo ad un laptop (forse addirittura il proprio) contenente dati top secret.]

A parte i paladini del "tanto io non ho niente da nascondere", chiunque altro **dovrebbe porsi parecchie, ma davvero parecchie, domande**.

Originally published at punto-informatico.it.

Scrivere a Cassandra—Twitter—Mastodon
Videorubrica "Quattro chiacchiere con Cassandra"
Lo Slog (Static Blog) di Cassandra
L'archivio di Cassandra: scuola, formazione e pensiero

By Marco A. L. Calamari on March 26, 2023.

Canonical link

Exported from Medium on August 27, 2025.